CHAPTER 4

Configuring the Cisco 2500 Series Access Server

This chapter describes the procedures for configuring the Cisco 2500 series access server and contains the following sections:

- Booting the Access Server for the First Time
- Using the Enable Secret and the Enable Password
- Configuring the Access Server

To configure your console, you need to connect a terminal to the access server. Configuration requires access to the console port.

If You Need More Information

The Cisco IOS software running the access server contains extensive features and functionality. The effective use of many of many of these features is easier if you have more information at hand. We recommend to you the following resources:

- UniverCD
- Cisco Information Online (CIO)
- Technical Assistance Center (TAC)

Additional Publications

For more information on configuring the Cisco 2500 series access server, see the appendix "Internetworking Primer," or refer to the following publications:

- *Access and Communication Servers Configuration Guide*
- *Access and Communication Servers Command Reference*
- *Configuration Builder Getting Started Guide*
- *Router Products Getting Started Guide*
- *Router Products Configuration Guide*
- *Router Products Command Reference*
- *Troubleshooting Internetworking Systems*

These publications are available on UniverCD.

All Cisco technical documentation and additional literature are available on UniverCD, Cisco's online library of product information. UniverCD is updated and shipped monthly, so it might be more up to date than printed documentation. UniverCD is available both as a single CD and as an annual subscription. To order UniverCD, contact your local sales representative or call Customer Service.

Contacting Customer Service

To obtain general information about Cisco Systems, Cisco's products or documentation, or upgrades, call 800 553-6387 or 408 526-7208. Customer Service hours are 5:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday (excluding company holidays). You can also send e-mail to `cs-rep@cisco.com`.

Using Cisco Information Online

Cisco Information Online (CIO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CIO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CIO provides a wealth of standard and value-added services to Cisco's customers and business partners. CIO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CIO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CIO (called "CIO Classic") supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CIO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CIO in the following ways:

- WWW: `http://www.cisco.com`.
- Telnet: `cio.cisco.com`.
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CIO's Frequently Asked Questions (FAQ), contact `cio-help@cisco.com`. For additional information, contact `cio-team@cisco.com`.

Contacting the Technical Assistance Center

If you are a system administrator and need personal technical assistance with a Cisco product which is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447 or 408 526-7209, or send an e-mail message to `tac@cisco.com`. Emergency technical assistance (for network-down or severe network problems) is available 24 hours a day, 7 days a week.

When you contact the TAC for help, have the following information ready:

- Chassis serial number
- Maintenance contract number

- Software version level and hardware configuration (enter the **show version** command to display this information)
- Software configuration (enter the **show running config** (Release 11.0 or later) or the **write terminal** command (Earlier than Release 11.0) to display this information)

Contacting the European Technical Assistance Center

Cisco and its European Service Partners coordinate all customer service in Europe, including hardware and software telephone technical support, onsite service, and module exchange and repair. For more information, contact the European TAC.

European TAC numbers and e-mail address are as follows:

- Phone: 32 2 778 42 42
- Fax: 32 2 778 43 00
- E-mail: `euro-tac@cisco.com`

Booting the Access Server for the First Time

The access server is administered using the Cisco command interpreter, called the EXEC. You must log in to the access server before you can enter an EXEC command. For security purposes the EXEC has two levels of access to commands, user EXEC mode and privileged EXEC mode.

To enter the privileged mode you must enter the enable secret password on systems running Cisco Internetwork Operating System (Cisco IOS) Release 10.2(3) or later, or the enable password on systems running Cisco IOS releases prior to 10.2(3) or when using the boot ROM monitor.

Using the Enable Secret and the Enable Password

The commands available at the user level are a subset of those available at the privileged level. Because many privileged-level EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use.

There are two commands you can use to do this, depending on the release you have of the Cisco IOS software:

- **enable secret** *password* (which is a very secure, encrypted password).
- **enable** *password* (which is a less secure, or nonencrypted, password).

The enable secret password is available in Cisco IOS Release 10.2(3) or later. The **e**nable secret password is not available before Release 10.2(3). The enable password is available in all releases. You must enter the correct password to gain access to privileged-level commands.

On systems running Release 10.2(3) or later, the enable secret password is used. when you are running from the boot ROM, the enable password might be used depending on your ROM level.

The passwords should be different for maximum security. If you enter the same password for both during the setup script, the system will accept it, but you will receive a warning message indicating that you should enter a different password.

An enable secret password can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an enable password can contain any number of uppercase and lowercase alphanumeric characters. In both cases, a number cannot be the first character. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored; trailing spaces are recognized.

If you lose or forget your enable password, see the section “Recovering a Lost Enable Password” in the chapter “Maintaining the Cisco 2500 Series Access Server.”

Configuring the Access Server

You can configure the access server following one of the procedures described in the following sections:

- Configuring the Access Server Using the Configuration Mode
- Configuring the Access Server Using AutoInstall
- Configuring the Access Server Manually Using the Setup Facility

Follow the procedure that best fits the needs of your network configuration.

Note You will need to acquire the correct network addresses from your system administrator or consult your network plan to determine correct addresses before you can complete the access server configuration. For details on network addressing, see the appendix "Internetworking Primer."

Before continuing the configuration process, check the current state of the access server by entering the **show version** command. The **show version** command will display the release of Cisco IOS software that is available on the access server.

Configuring the Access Server Using the Configuration Mode

You can configure the access server manually if you prefer not to use the setup facility or AutoInstall. Take the following steps to configure the access server manually:

Step 1 Connect a console terminal by following the instructions described in the section "Connecting the Console Terminal and Modem" in the chapter "Installing the Cisco 2500 Series Access Server" and then power up the access server.

Step 2 When you are asked if you would like to enter the initial dialog, answer **no** to go into the normal operating mode of the access server:

```
Would you like to enter the initial dialog? [yes]: no
```

Step 3 After a few seconds you will see the user EXEC prompt (Router>). Type **enable** to enter enable mode. Configuration changes can only be made in enable mode:

```
Router> enable
```

The prompt will change to the privileged EXEC prompt:

```
router#
```

Step 4 Enter the command **config terminal** at the enable prompt to enter configuration mode from the terminal:

```
router# config terminal
```

You can now enter any changes to the configuration that are desired. Press **Ctrl-Z** to exit configuration mode. (See the appendix "Internetworking Primer" for configuration assistance.)

To see the currently operating configuration, enter the command **show running-config** at the # prompt if you are running Cisco IOS Release 11.0 or later. Enter the command **write terminal** at the # prompt if you are running a Cisco IOS release earlier than 11.0:

```
router# show running-config
```

To see the configuration in NVRAM, enter the command **show startup-config** at the enable prompt.

```
router# show config
```

To make your changes permanent, enter the command **copy running-config startup-config** at the enable prompt if you are running Cisco IOS Release 11.0 or later. Enter the command **write memory** if you are running a Cisco IOS release earlier than 11.0:

```
router# copy running-config startup-config
********
```

The results of the **show running-config** and **show startup-config** commands will differ if you have made changes to the configuration, but have not yet written them to NVRAM.

The access server is now configured and will boot with the configuration you have entered.

Configuring the Access Server Using AutoInstall

The AutoInstall process is designed to configure the access server automatically after connection to your WAN. In order for AutoInstall to work properly, a Transmission Control Protocol/Internet Protocol (TCP/IP) host on your network must be preconfigured to provide the required configuration files. The TCP/IP host may exist anywhere on the network, as long as the following two conditions are maintained:

1. The host must be on the remote side of the access server's synchronous serial connection to the WAN.
2. User Datagram Protocol (UDP) broadcasts to and from the access server and the TCP/IP host must be enabled.

This functionality is coordinated by your system administrator at the site where the TCP/IP host is located. You should not attempt to use AutoInstall unless the required files have been provided on the TCP/IP host. See the publication *Access and Communication Server Configuration Guide* for information on how AutoInstall works.

Take the following steps to prepare your access server for the AutoInstall process:

Step 1 Attach the synchronous serial cable to the access server.

Step 2 Turn on power to the access server.

The access server will load the operating system image from Flash memory. If the remote end of the WAN connection is connected and properly configured, the AutoInstall process will begin.

If the AutoInstall completed successfully, you may wish to write the configuration data to the access server's nonvolatile random-access memory (NVRAM). Perform the following step to complete this task:

Step 3 At the # prompt, enter the **copy running-config startup-config** command if you are running Cisco IOS Release 11.0 or later, or the **write memory** command if you are running a Cisco IOS release earlier than 11.0:

```
Hostname# copy running-config startup-config
```

Taking this step will save the configuration settings that the AutoInstall process created in the access server. If you fail to do this, your configuration will be lost the next time you reload the access server.

Configuring the Access Server Manually Using the Setup Facility

If you do not plan to use AutoInstall, do not connect the access server's serial (WAN) cable to the channel service unit/data service unit (CSU/DSU). This will prevent the access server from attempting to run the AutoInstall process. The access server will attempt to run AutoInstall whenever you start it if the serial (WAN) connection is connected on both ends and the access server does not have a configuration stored in NVRAM. It can take several minutes for the access server to determine that AutoInstall is not set up to a remote TCP/IP host.

Once the access server has determined that AutoInstall is not configured, it will default to the setup facility. If the serial (WAN) cable is not connected, the access server will boot from Flash memory and go into the setup facility.

Note You can run the setup facility any time you are at the enable prompt (#) by entering the command **setup**.

Configuring the Global Parameters

When you first start the setup program you must configure the global parameters. The global parameters are used for controlling system-wide settings. Use the following procedure to enter the global parameters:

Step 1 Connect a console terminal by following the instructions in the section "Connecting the Console Terminal and Modem" in the chapter "Installing the Cisco 2500 Series Access Server" and then boot the access server to the EXEC prompt (Router>).

Step 2 When you have booted from Flash memory, the following information will appear after about 30 seconds. When you see this information displayed, you have successfully booted your access server:

```
System Bootstrap, Version 4.14(8), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 16384 Kbytes of main memory

Loading igs-c-l.110-0.7 at 0x3000040, size = 3865444 bytes [OK]

F3: 3779532+85880+173868 at 0x3000060
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
            cisco Systems, Inc.
            170 West Tasman Drive
            San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-C-L), Version 11.0(0.8), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Mon 19-Jun-95 23:22 by
Image text-base: 0x030200E4, data-base: 0x00001000

cisco 2500 (68030) processor (revision C) with 16380K/2048K bytes of
memory.
Processor board ID 2685538369
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software (copyright 1994 by TGV Inc).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Bridging software.
Authorized for Enterprise software set.  (0x0)
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
8 terminal lines.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read ONLY)

Notice: NVRAM invalid, possibly due to write erase.

         --- System Configuration Dialog ---


At any point you may enter a question mark '?' for help.
Refer to the 'Getting Started' Guide for additional help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

Step 3 Enter **yes** or press **Return** when you are asked if you would like to enter the configuration dialog and if you would like to see the current interface summary. Press **Return** to accept the default (yes):

```
Would you like to enter the initial configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:

Any interface listed with OK? value "NO" does not have a valid
configuration
```

```
Interface    IP-Address      OK?  Method     Status  Protocol
Ethernet0    unassigned      NO   not set    up      down
Serial0      unassigned      NO   not set    down    down
Serial1      unassigned      NO   not set    down    down
```

Step 4 Choose what protocols to support on your Ethernet or Token Ring interface. For IP-only installations, you can accept the default values for most of the questions. A typical configuration using IP, IPX, and AppleTalk follows:

```
Configuring global parameters:

  Enter host name [Router]: router
```

Step 5 Enter the enable secret password, the enable password, and the virtual terminal password:

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

  Enter enable secret : shovel

The enable password is used when there is no enable secret
and when using older software and some boot images.

  Enter enable password : trowel
    Enter virtual terminal password: pail
```

Enter **yes** or **no** to accept or refuse SNMP management:

```
  Configure SNMP Network Management? [no]:
```

The Simple Network Management Protocol (SNMP) is the most widely supported open standard for network management. It provides a means to access and set configuration and run-time parameters of routers and communication servers. SNMP defines a set of functions that can be used to monitor and control network elements.

Step 6 Determine if you will be using DECnet on your access server. If you are configuring for DECnet, enter the appropriate values for your area number, node number, and area routing:

```
  Configure DECnet? [no]:
```

Step 7 In most cases you will use IP routing. If you are using IP routing, you must also select an interior routing protocol. You can specify only one of two interior routing protocols to operate on your system using setup: Interior Gateway Routing Protocol (IGRP) or Routing Information Protocol (RIP).

Enter **yes** (the default) or press **Return** to configure IP, and then select an interior routing protocol for IP:

```
Configure IP? [yes]:
  Configure IGRP routing? [yes]:
    Your IGRP autonomous system number [1]: 15
```

Step 8 In this example, routing will be enabled on AppleTalk and IPX; IP has already been selected:

```
Configure AppleTalk? [no]: yes
    Multizone networks? [no]: yes

 Configure LAT? [yes]: no
 Configure IPX? [no]: yes
```

Configuring the Asynchronous Interface

The access server is equipped with up to 16 asynchronous interfaces, which are referred to as lines in the setup dialog. The asynchronous lines must be configured to permit asynchronous devices to be connected to the access server. (See the sections "Asynchronous Protocols," and "Modems" in the appendix "Internetworking Primer.")

The asynchronous ports on the access server are configured to allow connection by TTY devices, Remote nodes, and Remote LANs.

A variety of devices can connect to the access server using the asynchronous lines. Terminals and remote nodes (such as PCs, Macintosh computers, workstations, and host systems) connect to the access server and make use of its services. The access server provides services allowing access to other asynchronous devices, such as printers, modems, or terminals.

The following steps configure the lines on the access server to permit use of the asynchronous lines by the access server or remote devices:

Step 1 Enter **yes** or press **Return** to configure asynchronous lines:

```
Configure Async lines? [yes]:
```

Step 2 Set the line speed and the flow control for the asynchronous lines. Hardware flow control must be configured to allow proper communications with modems.

```
Async line speed [9600]:57600
Configure for HW flow control? [yes]:
```

For additional information on configuring modem connections see the section "Modems" in the appendix "Internetworking Primer."

Step 3 Enter **yes** if you will be connecting modems to your access server to allow remote sessions, and to configure your modems to use the default chat script:

```
Configure for modems? [yes/no]: yes
   Configure for default chat script? [yes]:
```

Step 4 Configure your system to allow serial line internet protocol (SLIP) and Point-to-Point protocol (PPP) access, as follows:

```
Configure for Dial-in IP SLIP/PPP access? [no]: yes
  Configure for Dynamic IP addresses? [yes]: no
  Configure Default IP addresses? [no]: yes
  Configure for TCP Header Compression? [yes]:no
  Configure for routing updates on async links? [no]:
```

For additional information on configuring SLIP and PPP connections, see the section "Asynchronous Protocols" in the appendix "Internetworking Primer."

Step 5 Enter **yes** or press **Return** at the AppleTalk remote access prompt to configure for AppleTalk, and then enter the AppleTalk network address and zone name for your AppleTalk clients.

```
Configure for Appletalk Remote Access? [yes]:
  AppleTalk Network for ARA clients [1]: 99
  Zone name for ARA clients [ara-dialins]:
```

ARA protocol uses an internal nonextended unique network number, and a zone name for ARA protocol clients. For additional information on configuring ARA protocol, see the section "Asynchronous Protocols" in the appendix "Internetworking Primer."

Step 6 Enter **yes** if you will be using IPX on your asynchronous lines, In this example, the access server will not be using IPX on the asynchronous lines:

```
    Configure XRemote font servers? [no]:
    Configure for Async IPX? [yes]: no
```

Configuring the Ethernet or Token Ring Interfaces

Take the following steps to configure the Ethernet or Token Ring interface to allow communication over a LAN. To configure the interface parameters, you need to know your Ethernet or Token Ring interface network addresses.

Step 1 In the following example, the system is being configured for an Ethernet LAN using IP. Respond as follows (using your own addresses and mask) to the setup prompts:

```
Configuring interface parameters:

Configuring interface Ethernet0:
  Is this interface in use? [yes]:
 Configure IP on this interface? [yes]:
    IP address for this interface: 172.16.72.1
    Number of bits in subnet field [0]: 8

   Class B network is 172.16.0.0, 8 subnet bits; mask is 255.255.255.0
```

Step 2 Enter **yes** if you will be using AppleTalk on the interface, enter **yes** to configure for extended AppleTalk networks, and then enter the cable range number. See the appendix "Internetworking Primer" for additional information on AppleTalk routing. Enter the zone name, and any other additional zones that will be associated with your local zone:

```
Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [no]: yes
    AppleTalk starting cable range [0]: 1
    AppleTalk ending cable range [1]: 2

    AppleTalk zone name [myzone]:
    AppleTalk additional zone name: otherzone
    AppleTalk additional zone name:
```

Step 3 Determine if you are going to enable IPX on this interface, enter the unique IPX network number. See the appendix "Internetworking Primer" for additional information on IPX routing:

```
Configure IPX on this interface? [no]: yes
    IPX network number [1]: B001
Configure XNS on this interface? [no]
```

Configuring the Synchronous Serial Interfaces

The synchronous serial interfaces are configured to allow connection to WANs through a CSU/DSU. Once the Ethernet or Token Ring port on your access server has been configured, take the following steps to configure the serial port:

Step 1 Enter **yes** to configure serial port 0:

```
Configuring interface Serial0:
  Is this interface in use? [no]: yes
```

Step 2 Determine what protocols you will allow on the synchronous serial interface and enter the appropriate responses:

```
Configure IP unnumbered on this interface? [no]: no
    IP address for this interface: 172.16.73.1
    Number of bits in subnet field [8]:
Class B network is 172.16.0.0, 8 subnet bits; mask is 255.255.255.0

Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [yes]:

    AppleTalk starting cable range [2]: 3
    AppleTalk ending cable range [3]: 3

    AppleTalk zone name [myzone]: ZZ Serial
    AppleTalk additional zone name:

Configure IPX on this interface? [no]: yes
    IPX network number [2]: B000
```

Step 3 Configure the second synchronous serial interface as follows:

```
Configuring interface Serial1:
  Is this interface in use? [no]:
```

```
Configure IP unnumbered on this interface? [no]: yes
    IP address for this interface: 172.16.74.2
    Number of bits in subnet field [8]:
Class B network is 172.16.0.0, 8 subnet bits; mask is 255.255.255.0

 Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [2]: 4
    AppleTalk ending cable range [3]: 4

    AppleTalk zone name [myzone]: ZZ Serial
    AppleTalk additional zone name:

 Configure IPX on this interface? [no]: yes
    IPX network number [2]: B002
```

Entering the Asynchronous Interface Addresses

After the asynchronous lines have been configured and the routing protocols have been selected, enter the IP addresses for each asynchronous interface.

For information on asynchronous protocols, see the section “Asynchronous Protocols” in the appendix “Internetworking Primer,” and for information on IP addressing, see the section “Desktop Protocols” in the appendix “Internetworking Primer.”

Step 1 Enter the IP address for each of the asynchronous interfaces on the access server:

```
Configuring interface Async1:
   Default client IP address for this interface [none]: 172.16.72.11

Configuring interface Async2:
    Default client IP address for this interface [172.16.72.12]:

Configuring interface Async3:
    Default client IP address for this interface [172.16.72.13]:

Configuring interface Async4:
    Default client IP address for this interface [172.16.72.14]:

Configuring interface Async5:
    Default client IP address for this interface [172.16.72.15]:
```

```
Configuring interface Async6:
    Default client IP address for this interface [172.16.72.16]:

Configuring interface Async7:
    Default client IP address for this interface [172.16.72.17]:

Configuring interface Async8:
    Default client IP address for this interface [172.16.72.18]:
```

Step 2 The configuration you have entered is now displayed and you are asked if you want to use the displayed configuration. If you answer **no**, you can begin the configuration again. If you answer **yes**, the configuration will be entered and saved in the startup configuration:

```
Use this configuration? [yes/no]:yes

Press RETURN to get started!

[OK]

Use the enabled mode 'configure' command to modify this
configuration.
```

The access server is now configured properly and is ready to use. Enter the command **setup** if you want to modify the parameters after the initial configuration. To perform more complex configurations, enter the command **configure**. For information on configuration, see the publication *Access and Communications Servers Configuration Guide*.

Checking Your Settings

You can check the value of the settings you have entered by entering at the # prompt the command **show running-config** if you are running Cisco IOS Release 11.0 or later, or the command **write terminal** if you are running a Cisco IOS Release earlier than 11.0:

```
router# show running-config
.
.
.
configuration register is 0x2102
```

To store the configuration or changes to your startup configuration, enter at the hostname# prompt the command **copy running-config startup-config** if you are running Cisco IOS Release 11.0 or later, or the command **write memory** if you are running a Cisco IOS release earlier than 11.0:

```
Hostname# copy running-config startup-config
```

Entering this command will save the configuration settings that the setup process created in the access server. If you fail to do this, your configuration will be lost the next time you reload the access server.